

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

L'e-gouvernement

De Terwangne , Cécile; Lobet-Maris, Claire; Pouillet, Yves

Published in:
Louvain

Publication date:
2007

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

De Terwangne , C, Lobet-Maris, C & Pouillet, Y 2007, 'L'e-gouvernement: aux armes, citoyens ?', *Louvain*, Numéro 166, p. 22-24.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

L'e-gouvernement : AUX ARMES, CITOYENS ?

L'e-gouvernement prône les outils technologiques au nom de l'efficacité administrative. Cependant, une autre valeur doit entrer en ligne de compte : la transparence, garante de la confiance du citoyen.

Dans le système traditionnel, le citoyen devait coordonner lui-même ses démarches administratives. La perspective introduite par l'e-gouvernement se propose de déplacer cette coordination vers l'administration, à travers une offre de services en ligne, intégrée et coordonnée. Mais guichets uniques, administrations en réseau, carte d'identité électronique et numéro d'identification unique sont-ils un simple changement de forme dans le mode de prestation des services publics ou un changement plus radical dont il convient d'interroger la signification sociale et politique pour nos libertés et notre vie privée ?

Guichet unique : la fin du labyrinthe

Qui n'a pas déjà entendu ces discours qui dénoncent le «parcours de combattants» de citoyens ou d'entreprises dans l'accomplissement de certaines procédures administratives ? À ce parcours morcelé, chaotique et souvent redondant, l'e-gouvernement entend répondre par le «guichet unique» : il s'agit d'une approche intégrée des procédures via le développement de lignes de vie, sorte de cheminements simplifiés et balisés du parcours du citoyen ou de l'entreprise dans ses démarches administratives. Ces approches proposent un découpage des relations administrations-citoyens en événements de vie (naissance, mariage, etc.), chacun orchestré par un back-office administratif dont le citoyen n'a plus à connaître les méandres.

L'image du citoyen tend à se réduire à celle d'un client ou d'un récepteur d'un produit administratif.

Cette approche en lignes de vie constitue un indéniable progrès. Du point de vue de nos libertés, elle n'en pose pas moins la question de la normativité sous-jacente à de telles réformes. Proposer des événements de vie aux citoyens comme aux entreprises suppose aussi de cadrer les relations citoyens-administrations dans un ensemble de parcours ou de scénarios



pré-normés qui balisent le champ des possibles. Plus la procédure est automatisée et intégrée, plus la normativité se fait forte. Elle réduit donc le champ des possibles du citoyen à ce qui a été programmé pour lui. Cela laisse peu de place à la liberté en dehors des parcours fléchés par l'administration. Ce regroupement par événement de vie traduit aussi la montée en puissance du paradigme consumériste dans la relation administrations-citoyens. L'image du citoyen tend à se réduire à celle d'un client ou d'un récepteur d'un produit administratif, très attentif à l'efficacité de son mode de délivrance. En témoignent les évolutions langagières : usager d'abord, client à présent, pour nommer celui qui n'aurait jamais dû perdre son titre ou statut de citoyen.

Ce réductionnisme dans l'approche des citoyens n'est pas sans poser question. Certes, l'efficacité est un critère important dans les relations avec l'administration. Mais la confiance dans les nouveaux systèmes qui se mettent en place en est un autre. Cette confiance passe par la transparence de l'usage fait par les administrations des données personnelles du citoyen. Sans cette transparence, on ne pourra pas empêcher que se crée ce paradoxe : le citoyen se trouvera face à une administration qui entend se rapprocher de lui, mais qui en même temps lui devient de plus en plus opaque.

Cette approche en lignes de vie et son mode de délivrance en guichet unique questionnent également les arrangements institutionnels qui président à l'organisation de ce nouveau mode de prestation de services.

Le rassemblement de multiples données sur un même support identifiant – la carte d'identité électronique par exemple – est une menace réelle pour les libertés des individus.



Traditionnellement, les administrations publiques étaient structurées en «silos» cloisonnés, indépendants les uns des autres. Cette image fragmentée de l'administration est aujourd'hui dénoncée comme l'anti-thèse de l'efficacité administrative. Et l'e-gouvernement entend le remplacer par un fonctionnement en réseau (*networked government*). Le réseau, plus encore depuis la métaphore de l'Internet, apparaît doté de vertus démocratiques d'autorégulation et de répartition des compétences, par opposition à l'image autoritaire et centralisée des modèles hiérarchiques de gouvernance publique. Or, ce qui se passe dans le domaine de l'e-gouvernement nous invite à une tout autre réalité d'une administration qui entend désormais se présenter comme un système d'information unique, parfaitement intégré et cohérent. Sans doute touche-t-on là plus au projet qu'à son déploiement effectif. Mais il convient toutefois de questionner cette vision dans ce qu'elle implique pour nos libertés et notre démocratie.

Quel équilibre des pouvoirs ?

La première question concerne l'équilibre des pouvoirs entre administrations et citoyens. L'abandon progressif du modèle en silos au profit d'une administration en réseau signifie aussi le renoncement à la garantie traditionnelle contre un État omniscient à l'égard duquel le citoyen serait totalement transparent¹. Ce renoncement doit être considéré avec lucidité, et non avec la certitude béate que tout progrès technique est bon en soi. Certes, il ne s'agit pas de tourner le dos aux technologies

Gendarmes et voleurs : une course sans fin

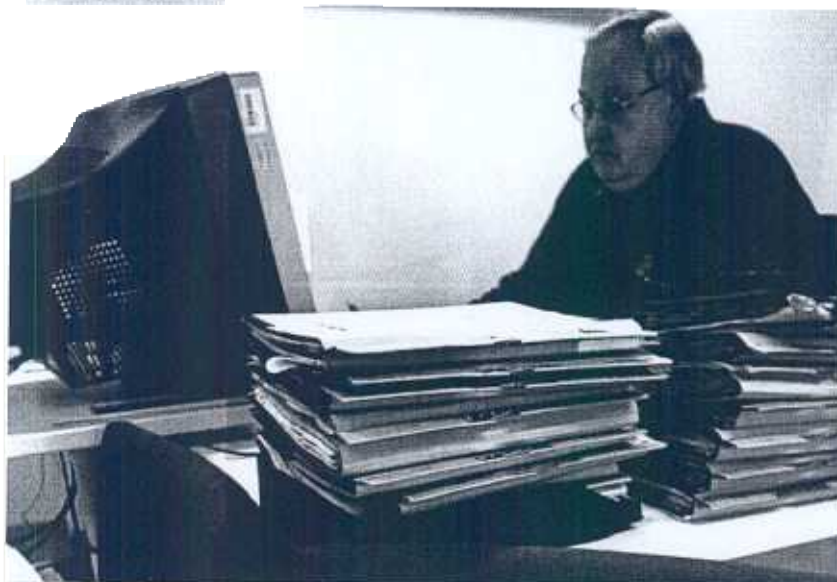
Signature électronique, carte SIS, vote magnétique, décodeur télévisé, carte de fidélité : autant d'outils de transport des données tantôt personnelles, tantôt d'utilité publique. Curieusement, il a fallu attendre le début des années 1990 (soit plus de dix ans après le lancement de la carte à puce en France) pour que la soi-disant inviolabilité de ces outils devienne un questionnement en soi, rappelle Jean-Jacques Quisquater, cryptographe à l'UCL. Jusque là, seul était de mise le discours sur la toute puissance de la technique, prôné par les autorités publiques et l'industrie : on utilisait des outils en postulant qu'ils permettaient une transmission parfaitement sécurisée des données ; on jurait que seules les personnes autorisées pouvaient avoir accès aux informations.

Or, explique le spécialiste international du chiffrement, «la sécurité absolue n'existe pas. Et même si elle existait, elle coûterait trop cher». Car protéger les systèmes demande des moyens. Mais les violer en demande davantage. Et que l'on soit gendarme ou voleur, cette escalade est sans fin. Les moyens de protection résultent donc toujours d'un compromis entre différents paramètres énumère M. Quisquater :

*«Paramètre financier : quel moyen a-t-on ?
Paramètre technique : l'industrie est-elle capable de suivre ? Et paramètre psychologique : comment l'utilisateur va-t-il réagir ? Après tout, sécuriser — mettre un mot de passe, par exemple —, c'est freiner l'usage. Quel frein le public est-il prêt à accepter ?»*

L'exemple de la télévision à péage illustre bien la balance entre ces différents éléments. Au début, ses initiateurs savaient très bien que le système n'était pas assez sécurisé. Un décodeur sur quatre a d'ailleurs été piraté. Mais c'était un risque assumé par le secteur audiovisuel : l'objectif était surtout d'amorcer la demande. Le raisonnement est tout à fait inverse en matière de commerce électronique. Pour que la vente en ligne tourne, il faut conforter la confiance de l'utilisateur. Le secteur bancaire doit donc investir dans des protections de haut niveau.

Reste que ces protections sont intrinsèquement faillibles, confirme Jean-Jacques Quisquater : «on peut seulement jouer sur la durée de vie : 5 ans au lieu de 3, par exemple, en fonction des moyens mis à disposition». Cette violabilité fondamentale n'est pas une question technique. Simplement, il est illusoire de croire que l'électronicien va penser à tous les usages possibles, présents et à venir. Or, si l'on ne prévoit pas tous les usages, forcément, l'on ne barre pas tous les accès. «Sécuriser, c'est prévoir le pire pour que le pire n'arrive jamais. Cela dit, je reste optimiste : malgré les possibilités de piratage et de sabotage, le système fait mieux que survivre», constate-t-il. Presque surpris. **Laurence Mundschau**



Reuters/Kristin Neumann

— À l'administration conçue comme un parcours du combattant, l'e-gouvernement répond par le «guichet unique», système qui balise les démarches administratives en les découpant par étapes.

nouvelles. Mais on ne peut pas réduire l'État à un simple fournisseur de services en quête d'efficacité. L'efficacité est assurément une valeur à promouvoir au sein des administrations publiques. Cependant, étant donné la quantité et la nature des données à caractère personnel traitées par le secteur public, et le caractère obligatoire de leur collecte, d'autres valeurs doivent intervenir.

La deuxième question relève de la transparence des traitements et des échanges d'information qui sous-tendent ce fonctionnement en réseau. Une des préoccupations affichées par les promoteurs de l'e-gouvernement est d'éviter les demandes répétées des mêmes informations auprès des citoyens ou des entreprises. C'est le principe de la collecte unique des données. Cela garantit une meilleure fiabilité et des bases de données dites «authentiques» (le registre national, la banque carrefour des entreprises, la documentation patrimoniale, etc.). Mais supprimer les demandes répétées d'une même information implique nécessairement un partage de cette information entre les entités publiques intéressées. Ce qui pose directement la question de la protection de la vie privée et des libertés du citoyen.

Trois principes doivent guider le cadrage démocratique de l'e-gouvernement. Le premier est le principe de finalité : une entité administrative peut avoir accès uniquement aux données nécessaires à l'accomplissement de ses obligations légales. Le deuxième est le principe de la juste proportionnalité entre les intérêts des sujets propriétaires des données et les intérêts des utilisateurs de celles-ci. Enfin, le dernier principe est celui de la transparence, garante de la confiance du citoyen : les aires de partage de l'information au sein des administrations doivent être claires et transparentes. Le droit d'accès du citoyen à ses données personnelles, consacré par la loi de protection des données à caractère personnel, peut aider à cette trans-

parence. À condition qu'on n'hésite pas à armer le citoyen des mêmes avantages de la technologie pour exercer ses prérogatives. Le droit d'accès pourrait, par exemple, s'opérer électroniquement et permettre de connaître l'état du dossier, les personnes qui y ont eu accès, l'origine des données obtenues par l'administration et la logique suivie lors d'une décision.

La troisième question est plus politique. On peut en effet se demander si l'e-gouvernement n'est pas en train de reconfigurer la donne de notre paysage institutionnel au profit de grands acteurs administratifs qui s'imposent d'autant plus facilement qu'ils sont fédéraux et détenteurs des bases de données authentiques. Certes, la question est prospective. Mais elle n'en amorce pas moins une tension dont il faudra pouvoir débattre entre l'ordre politique, où la démocratie se conjugue avec une saine répartition des pouvoirs, et l'ordre gestionnaire, où l'efficacité publique se conjugue avec l'intégration des systèmes administratifs.

Les sésames de l'e-gouvernement

On terminera ce propos en présentant les deux sésames de l'e-gouvernement.

La présentation de la carte d'identité électronique s'est faite sur un ton enthousiaste et prometteur d'efficacité : outil d'identification électronique infaillible, véritable sésame pour un ensemble toujours plus grand de services administratifs en ligne... Mais cette avancée technologique ne doit pas se réaliser sans réflexion sur les enjeux qu'elle suscite pour la vie privée et nos libertés démocratiques. Si la technique se révèle au point, cette carte aura vite tendance à être utilisée comme moyen systématique d'identification des personnes en ligne. Il importe donc de bien peser ce que l'on décide de faire apparaître sur la carte et les fonctions qu'on lui réserve. Est-il opportun, par exemple, de joindre un outil de paiement à la carte, ou le dossier médical, ou encore d'y inclure une puce de type RFID ? Le deuxième instrument est le numéro d'identification unique. L'attribution d'un «numéro national» à chaque citoyen depuis sa naissance n'est pas une nouveauté apparue avec l'e-gouvernement. La mise en réseau des différents départements administratifs, l'interconnexion des services créent toutefois un environnement dans lequel l'utilisation d'un identifiant unique a une portée bien plus large. Dans le contexte de l'e-gouvernement, le recours à un outil d'accès transversal aux données d'un individu présente un danger plus grand pour celui-ci du fait des croisements d'informations rendus possibles. Sans doute, les systèmes d'autorisation mis en place pour l'interconnexion de fichiers administratifs et reposant sur des comités sectoriels permettent-ils d'éviter le pire. Mais cette multiplication de comités sectoriels (on en compte déjà cinq et d'autres sont en projet) constitue aussi une dilution des responsabilités et n'aide pas à la clarté du fonctionnement des réseaux administratifs.

«*Bien informés, les hommes sont des citoyens, mal informés ils deviennent des sujets*», disait Alfred Sauvy. Une sagesse qu'il semble urgent de méditer sans quoi, pour paraphraser Philippe Quéau, la renaissance administrative promise grâce à l'e-gouvernement pourrait bien devenir le moyen âge des temps modernes avec ses nouvelles formes d'asservissement. ■

1. D. De Roy, C. de Terwangne, Y. Pouillet, «La Convention européenne des droits de l'homme en filigrane de l'administration électronique», in *50 ans d'application de la CEDH en Belgique: entre ombres et lumières*, Actes du Colloque organisé par le Centre de droit public de l'ULB les 20 et 21 octobre 2005 à Bruxelles, à paraître.